Towards a Federated SOA Model in Achieving Data Interoperability in DoD

Nick Duan, Ph.D.
ManTech-MBI
nduan@mcdonaldbradley.com

Abstract

The Department of Defense (DoD) is undergoing a progressive transformation towards a Net-Centric enterprise, and SOA has become a major enabling factor in driving the transformation. One of the major challenges facing many SOA-based programs in DoD is how to define a SOA model that is robust and scalable enough to meet mission-specific needs, while satisfying the Net-Centric requirements for data sharing across the multiple Services and Agencies in the Department. While there have been many SOA initiatives existed in DoD with various successes, data and service interoperability across multiple organizations are still limited due to lack of a coherent and overarching SOA model. In this paper, two different types of SOA models, a centralized and a fully distributed model, are discussed with respect to data interoperability and enterprise scalability. To achieve interoperability, a federated SOA model is introduced, along with a proposed strategy towards implementing a federated enterprise using the SOA principles. The identification and use of enterprise core services will be discussed, with respect to service discovery, security and support of disconnected operations. The benefits in data interoperability of the model and its applicability are demonstrated via a concrete case study on an existing Net-Centric program in DoD.

Acknowledgement

The concept presented in this paper is based on the work performed during the DCGS Interoperability Study. The author would like to express his sincere appreciation to members of the study team, especially Mark Day, Susan Lee, Chip Block, and MaryAnn Kiefer, for their comments and feedbacks that led to the completion of this paper.

1. Introduction

The Department of Defense (DoD) is undergoing a progressive transformation towards a Net-Centric enterprise, in support of data and service interoperability across various Services and Agencies to enhance mission-oriented decision making capabilities [1][4]. A major enabling factor of this transformation is the increasing adoption of Service-Oriented Architecture (SOA) and related products and services in many DoD programs. While many programs have achieved various success in SOA implementation at the Service/Agency level, data and service interoperability across multiple organizations are still limited due to lack of metadata understandability across COIs, monolithic core services providing centralized infrastructure functions, and enclave-specific, incompatible security policies. The main challenge remains on how to define and establish a coherent and overarching SOA model across multiple Services and Agencies, with sufficient infrastructure support to achieve large-scale data and service interoperability. Such a SOA model should encompass the necessary governance structure and service architecture, as well as the policies and processes for carrying out SOA implementations and conduct operations. Without an overarching SOA model, any large scale SOA implementation would remain a stove-piped experiment, and the grand vision of the Net-Centricity in sharing data and services would be difficult to realize.

In this paper, we introduce a federated SOA model in support of data and service interoperability in a multi-organizational enterprise. Compared with other types of SOA models, we believe that a federated SOA model is a viable and effective approach in establishing an ecosystem of self-organizing entities for sharing data and services. First, we will examine existing SOA models and

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
20 MAY 2008	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Towards a Federated SOA Model in Achieving Data Interoperability in DoD	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **ManTech-MBI**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
AFCEA-GMU C4I Center Symposium "Critical Issues In C4I" 20-21 May 2008, George Mason University, Fairfax, Virginia Campus, The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**23**	

highlight their pros and cons, with the emphasis on data and service discovery, information security, and support of disconnected operations. Second, we will define the basic concepts of the federated SOA model, discuss its suitability and benefits in supporting interoperability in large-scale enterprises, and address the design and SOA implementation issues, especially the use of enterprise core services. Third, we will demonstrate the benefits and applicability of the model via a concrete case study of the Distributed Common Ground Systems (DCGS), a major Intelligence, Surveillance, and Reconnaissance (ISR) data sharing initiative currently undergoing in DoD. Finally, we propose an implementation strategy towards achieving a federated SOA enterprise and conclude the paper with a summary of the federation concepts, as well as potential research tasks in this area.

2. The Challenges in Achieving Data and Service Interoperability

One of the major challenges facing many large programs in DoD is how to define a SOA model that is robust and scalable enough to meet mission-specific needs, while satisfying the Net-Centric requirements in support of data sharing across the Department. Most SOA implementations, based on commercial-off-the-shelf (COTS) products, are following a centralized SOA model that lacks the flexibility to provide loose-coupling among various service components, as well as the extensibility to scale enterprise services to the tactical level without compromising usability. Unlike commercial enterprises, DoD is not a truly single monolithic organization with a single funding source and a streamlined mission set, rather a conglomeration of entities with different funding lines and mission objectives. It would be extremely difficult to build a centralized SOA enterprise that satisfies everyone's needs, especially the needs of disconnected and/or disadvantaged users (i.e. field operations) at the tactical level. The centralized SOA approach wouldn't be a viable solution to the DoD's Net-Centric transformation due to the following reasons:

1. **Enterprise core services are centralized and difficult to extend beyond the enterprise level**. As defined in DoD's Net-Centric Service strategy, enterprise core services, such as service registry and discovery, content discovery and delivery, and enterprise security services, are essential in supporting data and service interoperability among service providers and service consumers. The current Net-Centric Enterprise Services (NCES) implementation, for instance, defines its enterprise core services in two Continental U.S. (CONUS) locations. It would be extremely difficult to scale and extend the availability of the centralized core services beyond the enterprise level to the tactical edge, especially to the war fighters who often conduct disconnected operations with low-bandwidth or without network connectivity.
2. **Centralized governance policies are not suitable to accommodate a wide range of mission categories.** In a centralized SOA implementation, SOA governance polices are generally defined at the highest enterprise level and maintained in a centralized repository. They are usually defined to accommodate operations in a well established, static environment, not suitable for operations in a less optimized, dynamic environment. For instance, the existing NCES security policy requires the use of Public Key Infrastructure (PKI) and the availability of static definitions of enterprise roles or attributes. In a tactical environment, the availability of PKI may not always be possible, and user access roles/attributes may change all the time based on war fighting scenarios.
3. **Centralized implementation using COTS products is not flexible in a tactical environment and limits real-time interoperability.** Current SOA implementation using the centralized approach is primarily based on commercial COTS products (such as J2EE and .Net-based products) that are designed for enterprise application integration with emphasis on heavy-duty transaction processing, rather than light-weight data and service interoperability. The complexity of Web Services stacks that most COTS products are based on, limits real-time data interoperability, thus making the COTS-based SOA implementation difficult to support operations at the tactical edge, due to multi-layer protocol stacks designed to deal with complex transaction and process control requirements. To support users in a tactical environment, a new approach in SOA implementation should be established to provide nimble and agile data interoperability with real-time constraints.

On the other end of the spectrum, a fully decentralized, distributed service model (e.g., the uncontrolled Web architecture on the Internet) would not be applicable to the Net-Centric environment, due to lack of governance, discoverability, command and control structure, and security between service providers and consumers. Most service and data activities occur in a peer-to-peer fashion, where

information is shared freely with little security and governance control. It would be extremely difficult to establish the necessary security mechanism required by the DoD to streamline authentication and access control over a vast variety of data assets and services. In addition, it would be difficult to support disconnected operations in a coordinated and streamlined fashion because information repositories are fully decentralized, and it is difficult to enable disconnected users to discover data or services on a temporal basis.

As an alternative, a *federation model* would make more sense conceptually in terms of enabling loose-coupling and autonomy among federation entities, while providing the scalability and the necessary governance control to ensure data sharing in a secure environment. A federated model is defined as a collection of self-organizing *federation entities*, and a set of governance rules and policies that provide oversight and control on interaction and collaborations among the federation entities. Each federation entity is able to retain control of its own internal activities, and to function autonomously. When applying the federation concepts to an organizational enterprise, the result is a *federated enterprise*. A *federated SOA model* is defined by constructing a federation model using SOA principles.

United States is a typical example of such a federated enterprise. As a federation entity, each State maintains its own autonomous legislation and decision making capability while collaborating and participating in the decision making process under the governance rules and policies of the federal government. In this environment, the primary nature of collaboration is information sharing, and the underlying business components and processes in support of the federation are loosely coupled, instead of tightly integrated. The same federation concept can be applied to the DoD environment, where multiple DoD Components, Services, or Agencies, each with their own specific mission objectives, business processes, and funding lines, are able to form a federated enterprise, with enhanced data and service interoperability in a loosely-coupled, collaborative, and secure environment.

Realizing the benefits of the federation model, the next step is to define the federation model in SOA terms to enable the implementation of a federated SOA enterprise. In the following section, we will discuss how a federated SOA model should be defined and constructed, as well as the essential design issues regarding service discovery, service security, and the support of disconnected operations, through the use of enterprise core services.

3. Achieving a Federated Enterprise using SOA

SOA as an information technology paradigm should be aligned with organizational governance structure to meet its value proposition. Since most command and control structures are hierarchical in general, we define the federated SOA model also as having a multi-level architecture. Most well-known federation models are defined in a hierarchical, multi-level fashion. A good example is the Domain Name Service (DNS), an Internet standard for organizing Internet Protocol (IP) addresses and mapping domain names. DNS enables domain name lookups by following the structured DNS hierarchy. Each organization may host its own DNS node and can function independently from others. The entire DNS consists of all individual DNS nodes distributed over the Internet. Each DNS node can operates independently from each other, yet is able to communicate and collaborate with each other to form a federation with unlimited scalability.

Following the DNS example, we define the federated SOA model as a set of loosely coupled, self-contained, individually managed *enclaves*, capable of exchanging data via interacting services by following standard protocols and governance policies. An *enclave* is defined in the context of information security in an enterprise. According to the DoD's Information Assurance (IA) standard, an enclave is a "collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves assume the highest mission assurance category and security classification of the applications or outsourced IT-based processes they support, and derive their security needs from those systems. They provide standard IA capabilities such as boundary C-3 defense, incident detection and response, and PKI key management. They also deliver common applications such as office automation and e-mail. Examples of enclaves include local area networks (and the applications they host), backbone networks, and data processing centers" [3].

We extended this definition of enclave to address the issue of interoperability, information security and support of disconnected operations. To support interoperability, an enclave representing a federating entity, is able to function as both a service provider and a service consumer. To support information security, each enclave is equipped with its own distinguished point of presence (POP), implemented

as a web server or enterprise portal running in a demilitarized zone (DMZ), and confined to standard security policies. A POP is responsible for access control of data to data resources and services hosted by the enclave. To support disconnected operations, an enclave is able to function in an autonomous fashion and capable to exchange information with the federation on a temporal basis. An enclave is also polymorphic in the sense that it may be comprised of multiple sub-enclaves, thus forming a multi-tiered structure. In this hierarchy, the top tier enclave represents the enterprise level, whereas the bottom tier represents the tactical level. Figure 1 shows how a federated SOA model is defined based on the definition of enclaves.

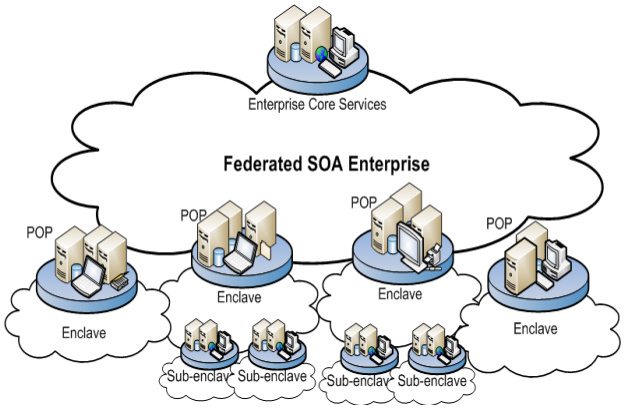


Figure 1. The Federated SOA Mode

Given the federation hierarchy of enclaves, interoperability can be achieved in two ways, horizontally and vertically. Horizontal interoperability deals with data and service exchange across enclave levels in any order, assuming that the necessary network connectivity is available. Vertical interoperability deals with information being propagated along the enclave hierarchy via *publish-up* and sync-down operations. Both publish-up and sync-down are necessary to support federated discovery, cross-enclave secure access, and disconnected operations.

Publish-up is the process of propagating information generated or collected from a lower-level enclave to the next higher level in a federation, similar to aggregating data content in a master-slave configuration. The type of information being propagated in this case is not restricted to registry and discovery, but could be any type of data, including metadata and actual content. The lower-level enclave, representing the publisher in this case, has the control on what data may be published.

Sync-down is the process of synchronizing or caching information in a lower-level enclave with information stored at the next higher-level enclave in a federated environment. The type of information is not restricted to registry and discovery, but could be any type of data, including metadata and the actual content. The lower-level enclave, representing the consumer in this case, has the control on what data to receive and cache.

Both horizontal and vertical interoperability ensures that data and services can be discovered and consumed across enclaves, and the mechanism to provide enclave with adequate information to perform disconnected operations. Each enclave can be considered as an autonomous unit, with its own data processes, services, and security policies. An enclave can join or leave the federation any time, depending on operational needs.

The hierarchical structure in federation maps well with the existing echelon and information processing structure of the DoD, allowing the adaptation and enforcement of governance policies and rules to be performed at each level. In a DoD C4ISR environment, for instance, a multi-level structure is defined for the ISR enterprise, from data capturing and collection, to information processing and dissemination. Currently, individual Services and Agencies have defined their ISR architectures in multiple layers. For instance, the Marines have defined levels as Fixed, Garrison, and Expeditionary; Army has defined levels ranging from Brigade Combat Team, Division, Corps, to CONUS; Navy has defined Afloat, Operation, and Strategic. Each level is defined by one or more enclaves that interact with each other via horizontal and vertical interoperability. The multi-level concept not only enables individual Services and Agencies to meet their operational needs, but also provides a way to structure information and align processes with organizational hierarchies. From a data asset management perspective, the structure of physical data assets is also arranged in a hierarchical fashion. Fixed, national/international data assets and core services will be offered by enclaves at higher levels in the hierarchy. Constrained/packaged data assets and flexible, mobile services will be offered by lower level enclaves.

4. The Use of Enterprise Core Services

Once we defined the structure and components of a federated SOA model, the remaining task would be to identify the federation behaviors, and create standards and processes for inter-enclave interactions in achieving data and service interoperability. By using enterprise core services at various levels of

federation, we will be able to define the federation behaviors to enable horizontal and vertical interoperability in a simple and consistent fashion.

Enterprise core services (in short, core services) are SOA-enabled Web Services that provide an service consumers and providers with standard and reusable infrastructure functions, such as service discovery, service security, and other supporting functions. They are the essential components in implementing the DoD's Net-Centric Service Strategy [6]. They are enterprise governance and control entities that form the backbone of the federation, providing the key components to ensure common SOA standards and governance policies are implemented, followed, and enforced.

Typical core services include service discovery, security, enterprise directory, messaging, collaboration, etc., such as those defined in the Defense Information Service Agency's (DISA) Net-Centric Enterprise Services (NCES) [2]. However, in the NCES world, core services are managed and operated only in a single level, enabling only horizontal interoperability at the top enterprise level, with limited scalability to extend service functions down to the tactical edge. To enable both horizontal and vertical interoperability, core services should be defined at multiple levels in a enclave to ensure the implementation success of a federated SOA model.

To create a loosely coupled enterprise with maximum agility to adopt and scale, the number of core services at the federal enterprise level should be kept at minimal. This is also necessary in order to avoid centralized control, and to maximize the flexibility and autonomy at the enclave level. To meet the interoperability requirements with respects to discovery, secure accessibility, and support of disconnected operations, only two basic core services should be established: registry/discovery (R/D) service, and security service. The former is necessary to enable data visibility across the enterprise, whereas the latter is required to enable data accessibility while enforcing the cross-enclave access policies. Both R/D service and security service will be discussed in subsequent sections.

5. Dynamic Discovery in a Federated Environment

The concept of R/D service is to enable registry and discovery of various data assets and services within a service-oriented enterprise. The establishment and availability of this core service is essential to enable visibility of data assets and services across enclaves. In addition to Web Services, an R/D service should support registration and discovery of other types of data services, including Representational State Transfer (REST), RSS channels, or simple Web sites. This is the first necessary step towards data interoperability because data assets should be made visible across the enterprise first, regardless of their readiness in understandability and accessibility.

To ensure that R/D services are interoperable among enclaves, industry open standards such as UDDI or ebXML are to be used to ensure platform-independence in a federated enterprise. The current industry standards for discovery do not deal directly with federated registry and discovery. To incorporate federation into registry and discovery, the publish-up and sync-down functions are to be used to enable cross-enclave discovery.

When fully federated, each enclave may host its own R/D service in support of disconnected operations. At the global enterprise level, one or more instances (in a high-availability, fault-tolerant configuration) of the R/D services may be established with aggregated registry contents from individual enclaves. Initially, data assets and services are to be registered locally within individual enclaves. The registry content of local or enclave-level registry will be propagated and aggregated with enclaves at the next tier via publish-up. The propagation and aggregation at higher levels continues until the registry entries are aggregated at the global enterprise level. Discovery of an asset can occur at multiple levels. If a consumer (human or machine) can't find the desired information at the local registry, the corresponding search query will be routed to the parent registry and the search continues. Local registries can cache the content of other registries to speed up the discovery process. Information discovered at a higher tier enclave is retrieved into a lower tier enclave where it can be cached locally via sync-down operations.

Although individual enclaves are hierarchical for registry and discovery federation, the communication for data or service access between two enclaves does not have to follow a hierarchical route. For instance, once a Marine unit discovers what certain Air Force ISR data services are available, it can communicate directly with these services. Similarly, the DNS structure does not have any direct impact on how IP traffic is routed between two computers. This federation architecture allows direct access of data and content information within the same tier or across tiers.

6. Secure Access in a Federated Environment

In addition to the R/D service, security service is also defined as another core service that is required in a federated enterprise. In general, security services deal with two security aspects, user authentication and authorization. User authentication is usually established via some PKI-based mechanism along with some federated identity management capabilities (to enable single-sign-on features) in an enterprise. Authentication and federated identity management is a topic by itself and is not within the scope of this discussion.

We focus our security aspect on user or consumer authorization in a federated environment. As a core service, a security service is defined primarily by an authorization policy service. If using role-based access control (RBAC) or attribute-based access control (ABAC) standard, the security service provides a lookup of the security role or attribute for a given user ID. The security policy service is necessary to ensure data access is enabled in a controlled manner in compliance with the necessary access policies across enclaves.

In a federated enterprise environment, each enclave is hosting its own security service, and is responsible for managing its own user information. User role or attribute information of an organization participating in the federation is to be identified and defined within the federating enclave where the primarily users are associated with. The user information may be propagated and exchanged along the federation hierarchy via the publish-up and sync-down processes. Cross-enclave data or service access is enabled when the access control information of remote users are cached in target enclaves. This information can also be cached locally in support of disconnected operations in which lower-level enclaves are detached from the corresponding high-level enclaves.

7. Case Study: Applying the Federated SOA Model to Distributed Common Ground Systems (DCGS)

DCGS is DoD's latest program to develop an integrated architecture of all ground/surface systems for sharing ISR information across all Military Services and the Intelligence Agencies. It is a portfolio consisting of multiple sub-programs or family members that are managed and funded by individual Services or Agencies, i.e. DCGS-Army, DCGS-Navy, DCGS-MC, DCGS-AF, and DCGS-IC. Each subprogram has developed or is in the process of developing its own SOA-based DCGS-XX architecture based on Services or Agencies specific requirements and mission objectives. Data interoperability across Services/Agencies remains an unsolved issue with increased complexity as the number of data assets and services offered increases, combined with incompatibility of architectures based on different COTS products and standards of core services.

A 90-day DCGS Interoperability Study [7] conducted last year by a multi-task force team in which the author was key member, revealed that the DCGS program should be better approached as a federated enterprise using a federated SOA model, because each DCGS sub-programs are loosely coupled in a distributed structure, and each Service or Agency maintains its own requirement and funding line.

As shown in Figure 2, DCGS can be defined as a federated SOA model consisting of multiple DCGS family members (e.g., DCGS-Army, DCGS-Navy, DCGS-AF, etc.). Each member represents a federating entity with its own autonomy, and is constructed as an enclave with its own Point-of-Presents (POP) to interact with the federation. Each federating entity itself is an enterprise with its own mission objectives and requirements to satisfy. Each one may have a different set of ISR data consumers, business rules, and ISR processes that differ from other entities. By managing and running each entity independently and autonomously, each entity is able to serve its customers in a unique way, leverage its own existing infrastructure and services, and achieve its mission objectives.

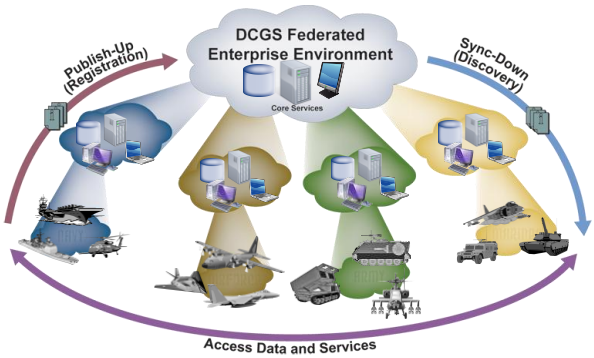


Figure 2. DCGS as a Federated Enterprise

Horizontal and vertical interoperability are achieved thought the use of core services to be

deployed at multiple levels along the federation hierarchy in support both publish-up and sync-down operations. The publish-up and sync-down capabilities of core services are also essential for enabling interoperability in disconnected operations. Some entities in DCGS are required to function in a disconnected, autonomous fashion because they operate only with temporary connectivity. For instance, a Marine Corps Expeditionary unit at the tactical edge may have to function independently without any network connectivity for an extended period of time. The publish-up and sync-down functions allow the unit to obtain the necessary information, or a Naval submarine is capable of downloading needed information from the enterprise, and uploading its own ISR data collection to the enterprise via satellite link, during a short period time on surface. After submerging, it will continue operating autonomously.

8. Strategy for Implementing the Federated SOA Model

A successful implementation of the federated SOA model relies on the right governance framework and implementation strategy. SOA governance deals with both organizational policies and technical standard and frameworks in establishing an enterprise environment for carrying out the SOA implementation. We define an implementation strategy consists of near-term, mid-term, and long-term goals that enable the creation of a federated enterprise through a measured and controlled process.

Depending on individual organization's readiness for SOA transformation and funding availability, the near-term, mid-term, and long-term goals can be defined with an estimated 6 months, 12 months, and 24 months period of performance for each of the three goals, respectively. The near-term goal is aimed at establishing the initial SOA capability with emphasis on horizontal data interoperability at the enterprise level. This requires the identification of the initial set of enclaves, and visibility of data and services via the use of service discovery core service. The mid-term goal is designed to achieve vertical interoperability within the enterprise, by pushing the data accessibility from the enterprise level to the tactical edge with selected mission threads. The long term goal is achieved via the enablement of both horizontal and vertical interoperability within the federated enterprise, as well as the establishment of a metadata framework for semantic understandability, in achieving the highest level of data interoperability in a Net-Centric environment [4][5].

9. Conclusions

In this paper, we discussed the basic concept of data interoperability in a large enterprise environment and proposed a federated SOA model in achieving Net-Centric data sharing in DoD. Compared with other architecture approaches, a federated SOA model is a sound and viable solution in enabling cross-enclave data and service interoperability in a multi-organizational enterprise. Both horizontal and vertical interoperability can be achieved via the use of core services that supports data and service discovery, secure access, and autonomous disconnected operations of enclaves. A federated enterprise consists of multiple, independent, and self-organizing enclaves as federating entities, constructed in a multi-level hierarchy that maps well with the organizational command and control structure in the DoD. Defining the enclaves in a polymorphic setting allows the federation model to be scalable and extensible beyond a single layer of enterprise.

Two basic types enterprise core services, R/D and security services, are to be established at each enclave level in a federation, to ensure standard compliance and enforce of governance policies for cross-enclave discovery and accessibility. Two essential core service capabilities, publish-up and sync-down, are defined as part of the federation framework to enable both horizontal and vertical interoperability, as well as to support disconnected operations.

A good understanding of the federated model will lead to the development of a new methodology of SOA implementations of large scale enterprises in the public sector and large corporations, since most large organizations have or prefer to have a loosely coupled management and funding structure. Future research tasks in this federated enterprise area may include identifying governance standards and processes of forming, joining and leaving a federation, as well as detailed process and protocols for implementing publish-up and sync-down operations.

10. References

[1] DoD Net-Centric Data Strategy, DoD CIO, May 9, 2003

[2] Defense Information Systems Agency. Core Enterprise Services, March 28, 2007, http://www.disa.mil/nces/enterprise_services.html

[3] DoD Directive Number 8005.01, Information Assurance (IA), ASD(NII)/DoD CIO, October 24, 2002

[4] DoD Directive Number 8320.02, Data Sharing in a Net-Centric Department of Defense, DoD CIO, December 2, 2004

[5] DoD Information Sharing Strategy, DoD CIO, May 4, 2007

[6] DoD Net-Centric Services Strategy, DoD CIO, May 4, 2007

[7] ManTech MBI, Distributed Common Ground System (DCGS) Interoperability Study Report for the DCGS Integration Backbone (DIB) Management Office (DMO), Jan. 11, 2008

[8] Thomas Erl, SOA Principles of Service Design, Prentice Hall, July, 2007

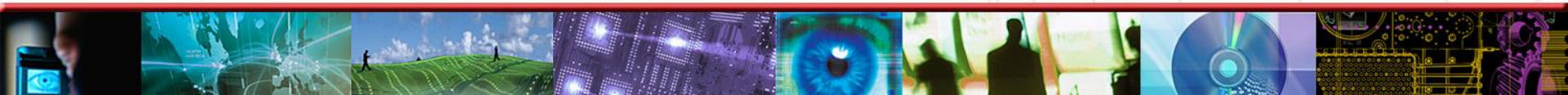
Biography

Dr. Nick Duan has over 20 years experience in applied research, enterprise software design and development. He has a wide range of knowledge and expertise in distributed enterprise computing, SOA, Web Services, J2EE, and enterprise security. He is currently a Sr. Software/SOA Architect with ManTech MBI, leading the SOA core competency effort of the company. A Sun Certified Enterprise Architect for the J2EE platform, Dr. Duan has worked with leading companies in the Hi-Tech industry, including Bell-Atlantic, webMethods, Northrop Grumman, SAIC, and McDonald Bradley. A graduate from The Penn State University and The Technical University of Aachen, he has published papers in various journals and conferences. He has taught computer language and software engineering courses as an adjunct faculty with local universities since mid 90s. He has been an adjunct faculty member with the Software Engineering Dept of GMU since 2003.

ManTech
International Corporation

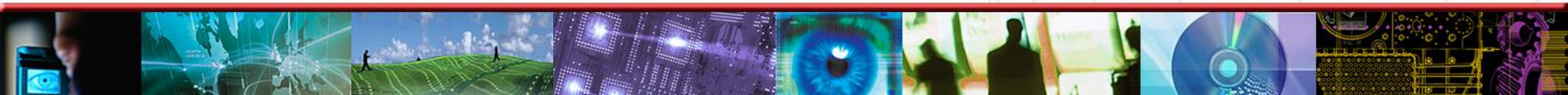
Towards a Federated SOA Model in Achieving Data Interoperability in DoD

Nick Duan, Ph.D.
ManTech MBI
AFCEA/GMU C4I Symposium
May 20, 2008



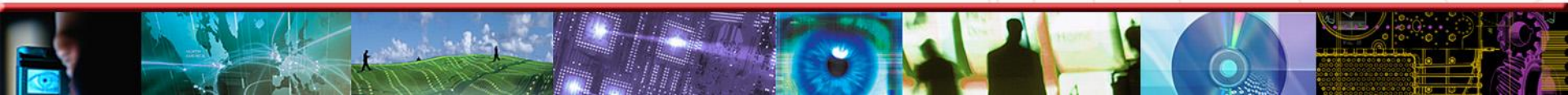
Overview

- The Interoperability Challenge and Use of SOA
- Existing SOA Models for Large-Scale, Multi-Organizational Enterprises
  - Centralized Model
  - Fully-Distributed, Peer-to-Peer Model
- The Federated SOA Model
- Achieving Inter-enclave interoperability via federation
- Case Study (Distributed Common Ground System)
- Conclusions



The Interoperability Challenge

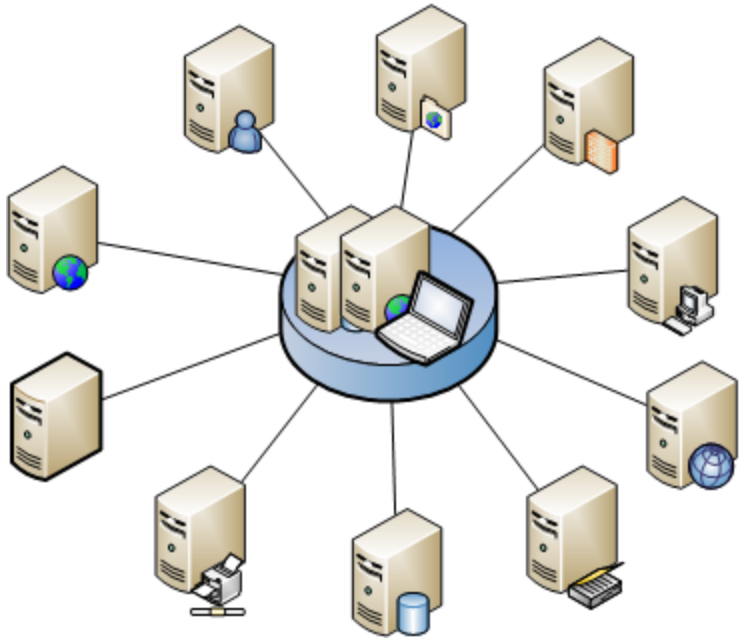
- Interoperability as the Key Component in Net-Centric Data Sharing
  - Visibility: Data and Service Discovery, Registry
  - Accessibility: Secure Access, Data Availability Anytime, Anywhere (support of disconnected ops)
  - Understandability: Metadata, Semantic Functions
- Interoperability in a Multi-Organizational Enterprise
  - Different mission focuses
  - Different funding sources
  - Different infrastructure, standards, governance policies
  - Need to balance between structured C2 and autonomy
- Commercial SOA models do not satisfy the needs



Common SOA Models for Implementing Large-scale Enterprises

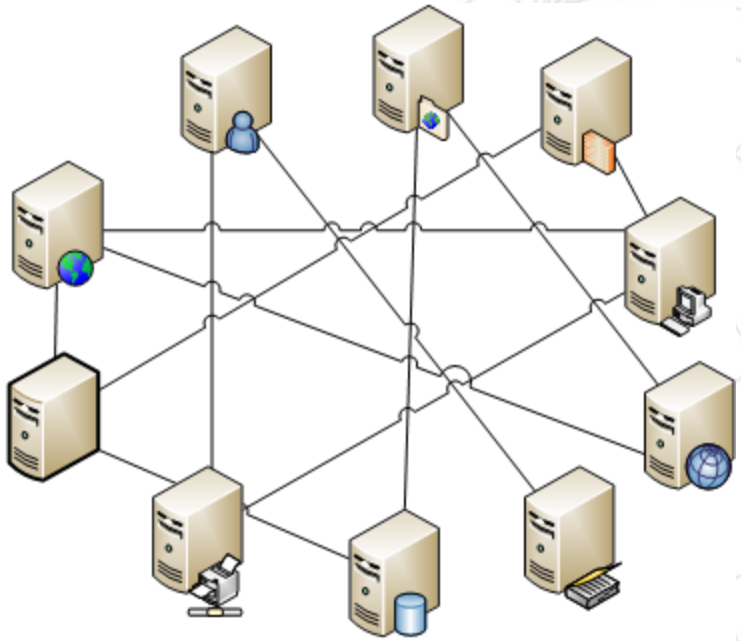
- Centralized Model

Core services are centralized and difficult to scale and extend, lacks extensibility for the tactical environment



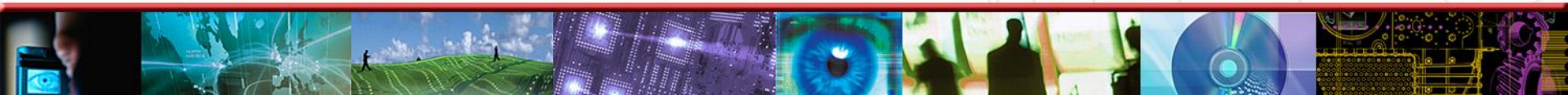
- Fully-Distributed, P2P Model

Lack of governance, discoverability, command and control structure, and the necessary security between service providers and consumers



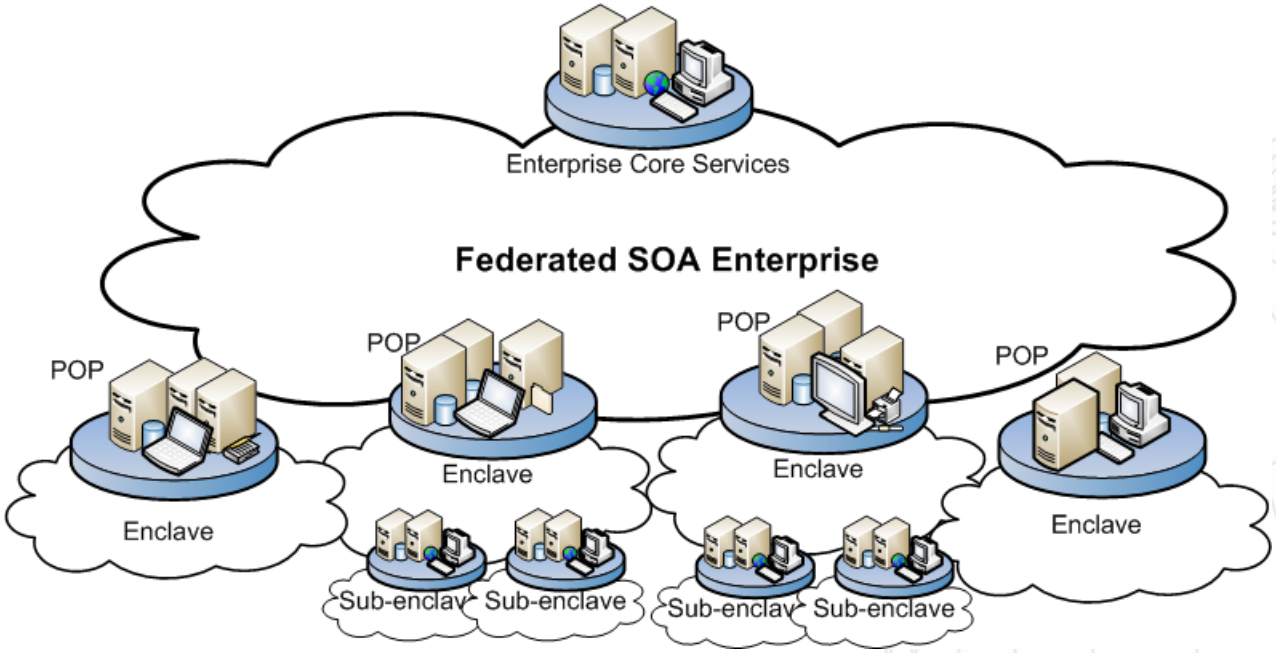
Alternative: Federation Model

- A typical multi-organizational environment is federated
- Model Definition: (Model Structure and Components)
  - a set of loosely coupled, self-contained, individually managed *enclaves,* capable of exchanging data via interacting services by following standard protocols and governance policies, and functioning as independent autonomous units
  - From an network/IA perspective, an enclave is collection of computing entities interconnected through an internal network and enclosed from the outside network
  - The interface of an enclave to the outside world is usually defined via a single point of presence (POP) (e.g. a web portal)
- Polymorphism of Enclaves
  - An enclave can comprise of multiple sub-enclaves
  - Hierarchical federation structure (for instance, DNS)



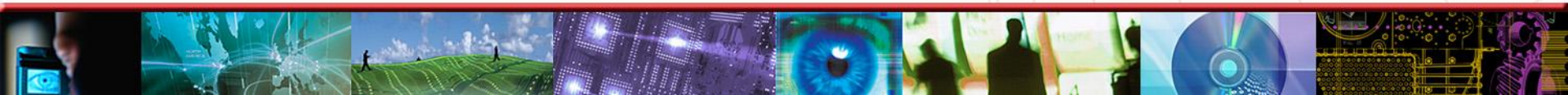
The Federated SOA Model

- Implementing the federation model using SOA technologies
- Two basic core services are defined: registry/discovery, security



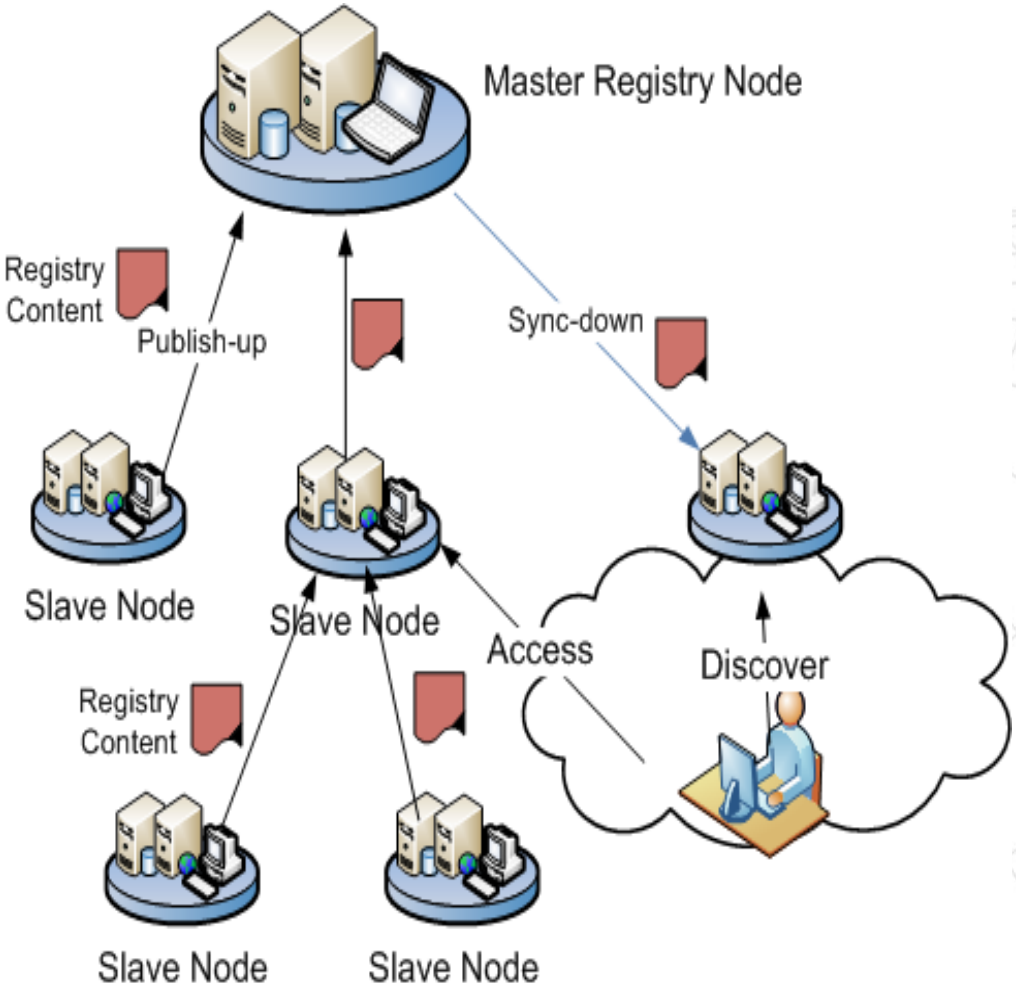
Inter-enclave Interoperability in a Federation

- Visibility/Discoverability
  - Each enclave is equipped with its own registry and discovery service to allow service registration and discovery at the enclave level
- Accessibility/Access Control
  - Each enclave is responsible for defining and maintaining its own access control policies
  - Enclave POP is the entry point for Inter-enclave accessibility
  - A set of global user roles or attributes are to be established to enable inter-enclave role mapping
- Support of Disconnected Operations
  - Each enclave is able to function as an autonomous unit



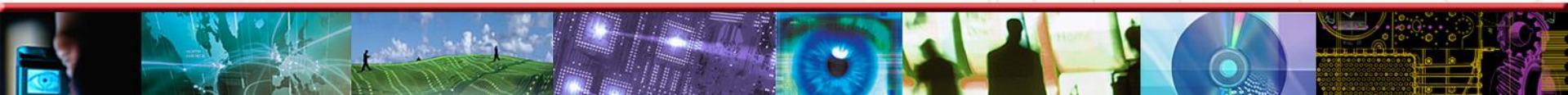
Federated Registry

- Federated registry is defined as a set of master/slave registry nodes in a federation hierarchy
- Registry content of a slave is to be replicated on the master via publish-up operations
- Registry content or partial content of a master can be cached on a slave via sync-down operations

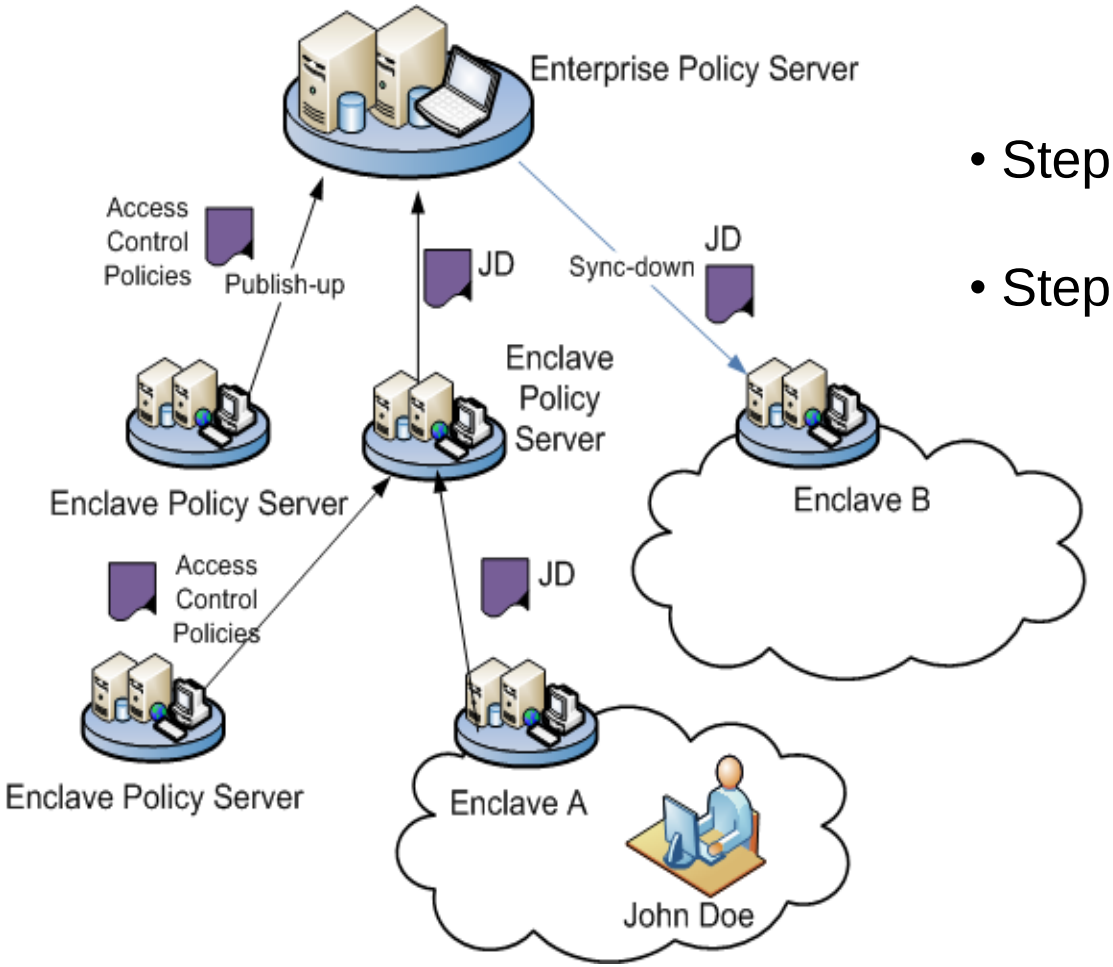


Federated Security

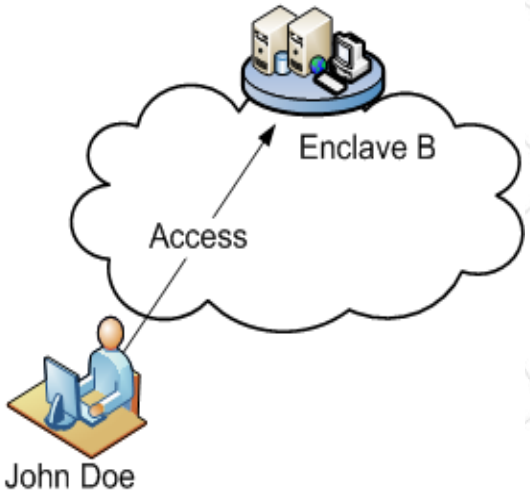
- Enterprise identity management solutions may be leveraged for connected operations
  - Establishing trust among enclaves
  - Using SAML/WS-Security to enable cross enclave accessibility
- Access control information of other enclaves is to be cached for disconnected operations
  - User identity and authorization policy info is cached locally within enclaves
  - Standard user roles/attributes are to be established to enable cross domain role mapping



Accessibility in Disconnected Operations

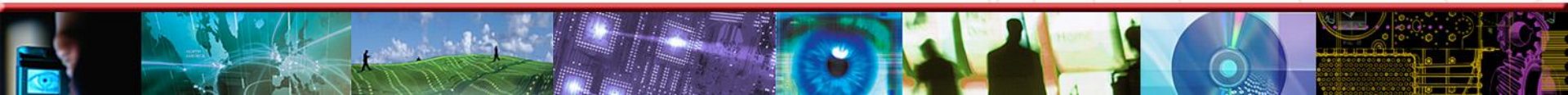


- Step 1: Sync-down user ID and policy info
- Step 2: User access



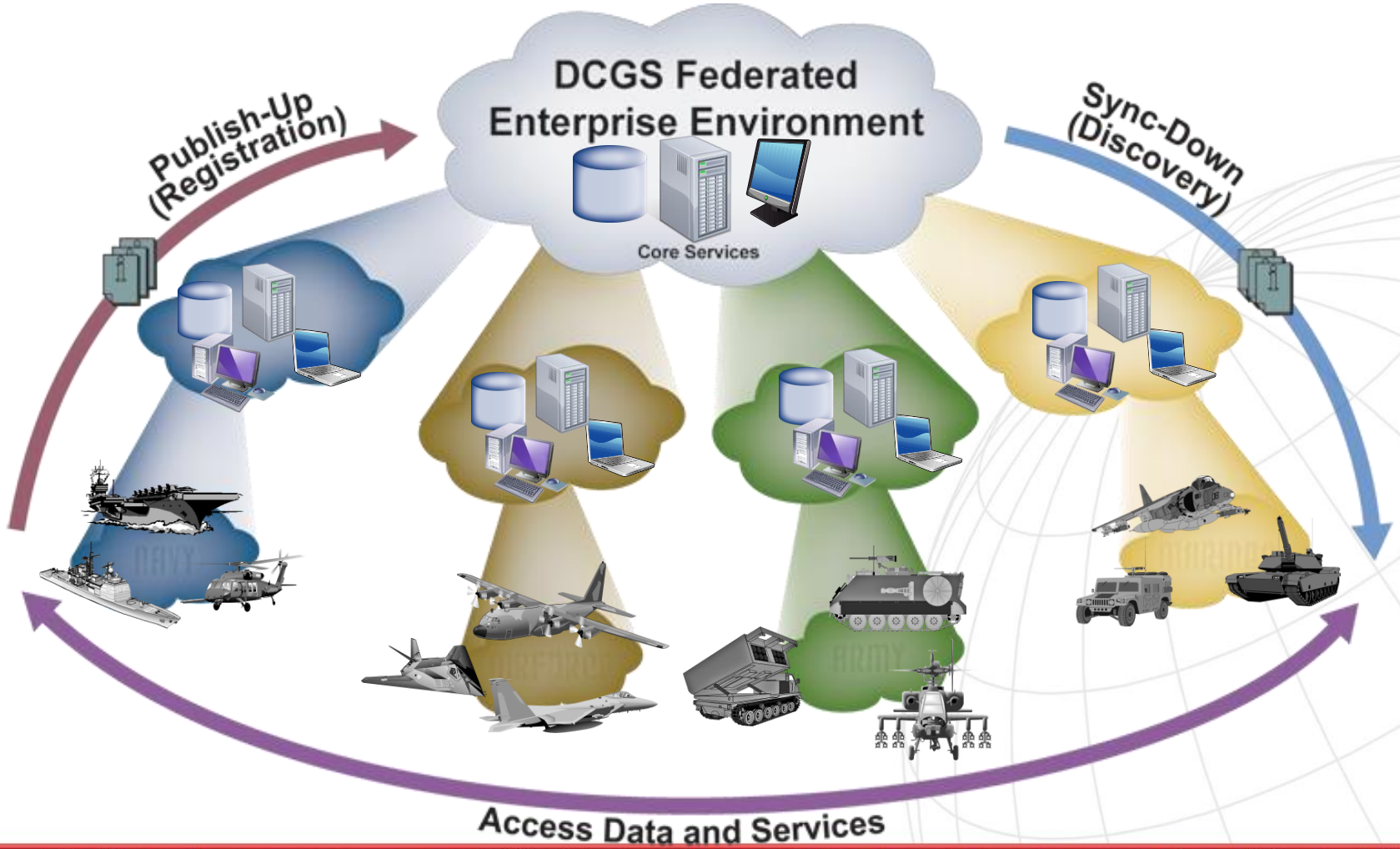
Case Study of Applying the Federation Model

- Distributed Common Ground System
  - A portfolio of systems to support ISR data processes across multiple DoD Components, Services, and Agencies, including DCGS-AF, DCGS-Army, DCGS-Navy, DCGS-MC, and DCGS-IC
  - Each DCGS member uses different standards and processes for ISR data processing and operations, and has various SOA implementations
  - Interoperability is limited, especially at the tactical level
  - Capability of pushing ISR data to tactical edge is highly desired, as well as support of disconnected operations



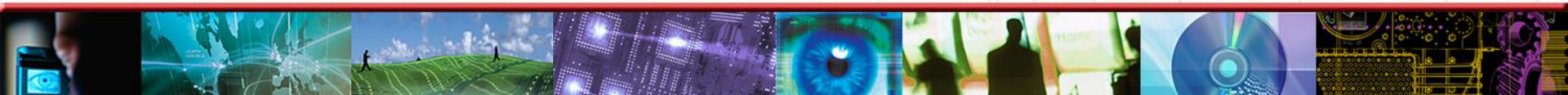
The DCGS Federated Enterprise

Achieving Interoperability via Federation



Conclusions

- The federated SOA model is a sound and scalable solution in enabling cross-enclave data and service interoperability in a multi-organizational enterprise
- Federated registry and federated security are to be implemented as core services in the federation to support visibility, accessibility and disconnected operations
- Future tasks on improving enterprise federation
  - Governance standards and policies on federation processes and procedures for forming, joining, and leaving a federation
  - Standards and protocols for publish-up and sync-down operations (content-staging in a federated environment)



Q&A